PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-008851
(43)Date of publication of application : 12.01.1996

(51)Int.Cl.	H04H 1/00
	H04L 9/00
	H04L 9/10
	H04L 9/12

(21)Application number : 06-134667
(22)Date of filing : 16.06.1994

(71)Applicant : TOSHIBA CORP
(72)Inventor : SHINPO ATSUSHI
KAMITAKE TAKASHI
MAEDA KENICHI

(54) INFORMATION DISTRIBUTION SYSTEM AND INFORMATION DISTRIBUTION METHOD

(57)Abstract:

PURPOSE: To provide an information distribution system capable of performing a primary and a secondary distribution of paid information and preventing damage from reaching equipments other than the terminal equipment even when the physical safety of the terminal is not guaranteed any more.

CONSTITUTION: In this information distribution system for distributing digital information from a supply station 101 to the plural terminals 103 among the terminals 103 through an information transmission medium, the supply station 101 is provided with a means for outputting ciphered information for which the information is ciphered by a first cryptographic key intrinsic to the respective pieces of the information and a distribution key for which a first deciphering key corresponding to the first cryptographic key is ciphered by a second cryptographic key intrinsic to a reception terminal to the medium. The respective terminals 103 are provided with the means for inputting the ciphered

information and the distribution key transmitted from the supply station 101 or the other terminal through the medium, the means for deciphering the ciphered information by the first deciphering key extracted by deciphering the distribution key by a second deciphering key corresponding to the second cryptographic key, the means for ciphering the first deciphering key extracted by deciphering the encipherment distribution key by the second deciphering key by the second cryptographic key intrinsic to the terminal which is the transmission destination of the ciphered information and the means for outputting the distribution key obtained by the means and the ciphered information to the medium.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] While consisting of signal transduction media which connect between the information supply station which distributes digital information, two or more information terminals which receive said digital information, and said information supply station and said two or more information terminals In the information distribution system which distributes said digital information distributed from said information supply station between each information terminal in 2nd order said information supply station The encryption digital information which enciphered this digital information using the 1st cryptographic key assigned to the proper for said every digital information, It has a means to output the encryption distribution key which enciphered the 1st decode key corresponding to this 1st cryptographic key using the 2nd cryptographic key assigned at the proper to said information terminal which should transmit this encryption digital information to said signal transduction medium. An input means by which said each of information terminal inputs said encryption digital information transmitted through said signal transduction medium from said information supply station or said other information terminals, and said encryption distribution key, A decode means to decode said encryption digital information using said 1st decode key obtained by this decode after decoding said encryption distribution key using the 2nd decode key of the proper corresponding to said 2nd cryptographic key, After decoding said encryption distribution key using said 2nd decode key, said 1st decode key obtained by this decode An encryption distribution key conversion means to encipher using said 2nd cryptographic key assigned at the proper to said another information terminal which should transmit said encryption digital information, The information distribution system characterized by having an output means to output said encryption distribution key obtained by this encryption distribution key conversion means, and said encryption digital information to said signal transduction medium.

[Claim 2] An edit means for said each of information terminal to edit said encryption digital information acquired by said decode means, An available frequency information storing means to store the available frequency information updated whenever it uses the digital information decoded by said encryption digital information or said decode means, While generating record of the use information according to the decode action of said encryption digital information by said decode means, and the edit action of said digital information by said edit means The information distribution system according to claim 1 characterized by having further the use management tool which updates said available frequency information stored in said available frequency information storing means according to said decode action and said edit action.

[Claim 3] Said decode means and said encryption distribution key conversion means are an information distribution system according to claim 1 characterized by being prepared in the field physically

protected from the exterior.
[Claim 4] While consisting of signal transduction media which connect between the information supply station which distributes digital information, two or more information terminals which receive said digital information, and said information supply station and said two or more information terminals In the information distribution system which distributes said digital information distributed from said information supply station between each information terminal in 2nd order said information supply station The 1st cryptographic key assigned to the proper for said every digital information The encryption distribution key which enciphered the 1st decode key corresponding to this 1st cryptographic key using the 2nd cryptographic key assigned at the proper to said information terminal which should transmit the encryption digital information which used and enciphered this digital information, and this encryption digital information, It has a means to output only this encryption distribution key to said signal transduction medium. Or said each of information terminal Said encryption digital information transmitted from said information supply station through said signal transduction medium, and said encryption distribution key Or an input means to input said encryption distribution key transmitted from said encryption digital information transmitted from said other information terminals, and said information supply station, A decode means to decode said encryption digital information using said 1st decode key obtained by this decode after decoding said encryption distribution key using the 2nd decode key of the proper corresponding to said 2nd cryptographic key, The information distribution system characterized by having an output means to output said encryption digital information to said signal transduction medium.
[Claim 5] Said information supply office is further equipped with a means to record the distribution action of said encryption distribution key to said each of information terminal. Said each of information terminal The edit means for editing said encryption digital information acquired by said decode means, An available frequency information storing means to store the available frequency information updated whenever it uses the digital information decoded by said encryption digital information or said decode means, While generating record of the use information according to the decode action of said encryption digital information by said decode means, and the edit action of said digital information by said edit means The information distribution system according to claim 4 characterized by having further the use management tool which updates said available frequency information

stored in said available frequency information storing means according to said decode action and said edit action.

[Claim 6] Said decode means is an information distribution system according to claim 4 by which it is characterized [which was prepared in the field physically protected from the exterior].

[Claim 7] In the information distribution approach of distributing the digital information which the 1st information terminal received while receiving distribution of digital information to the 2nd information terminal in 2nd order The encryption digital information which enciphered this digital information using the 1st cryptographic key assigned to the proper for said every digital information, The input step which inputs the encryption distribution key which enciphered the 1st decode key corresponding to this 1st cryptographic key using the 2nd cryptographic key assigned to said 1st information terminal at the proper, The decode step which decodes said encryption distribution key using the 2nd decode key of the proper corresponding to said 2nd cryptographic key, The encryption step enciphered using said 2nd cryptographic key to which said 1st decode key obtained by this decode step was assigned by said 2nd information terminal at the proper, The information distribution approach characterized by having the output step which outputs said encryption distribution key obtained at this encryption step, and said encryption digital information.

[Claim 8] In the information distribution approach of distributing the digital information which the 1st information terminal received while receiving distribution of digital information to the 2nd information terminal in 2nd order The 1st cryptographic key assigned to the proper for said every digital information The input step which inputs the encryption distribution key which enciphered the 1st decode key corresponding to this 1st cryptographic key using the 2nd cryptographic key assigned at the proper to the encryption digital information which used and enciphered this digital information, and said 1st information terminal, The information distribution approach characterized by having the step which performs at least one side of the processing which outputs the processing which decodes said encryption distribution key using the 2nd decode key of the proper corresponding to said 2nd cryptographic key, and said encryption digital information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to the information distribution system and the information distribution approach the perusal and editing become possible for a user in circulation of the digitized work, guaranteeing an author's right.

[0002]

[Description of the Prior Art] It is becoming possible to digitize various information, such as an image, voice, and a text, and to deal with it integrative by development of digital communication in recent years, a calculating-machine technique, etc. Some systems by which an information user can receive works, such as a newspaper by which installation is considered by each Field of application, for example, such a technique was digitized in the field about information distribution, a magazine, music, a movie, and --, through a network are proposed.

[0003] However, if it is actually going to build this kind of information distribution system, the important problem of protection of copyrights will actualize. That is, there is an outstanding point which can moreover create a perfect duplicate to an inexhaustible supply easily as a description it is featureless to analog information in the digital information treated by the above-mentioned system. Although this is a big advantage for a user, for the side which offers a work, it is a problem in respect of right protection. Therefore, in order to make the above-mentioned system perfect, the structure from which copyright can moreover be protected, without spoiling the description of digital information becomes indispensable.

[0004] Such a problem is already generated in distribution of the software (program) which can be said also as the forerunner of onerous digital information. And since there is a limitation naturally only by leaving protection of copyrights to regulation by law, the technical cure is worked on. Hereafter, two cures taken in distribution of software for protection of copyrights are explained.

[0005] The 1st approach is an approach of changing and distributing software to the format which can be performed only by the specific computer. Namely, while assigning ID of a proper to a computer, a user's computer ID is woven into selling software at the time of sale of software. Computer ID is compared with ID in software, and if not in agreement, it is made not to be started at the time of activation of software. However, only by writing a computer ID code in a part of software, if even the write-in location is known, protection will be broken simply. Then, a code technique is used as dilation, the whole software is enciphered with a certain key, and the method of customizing and distributing the key for every computer according to individual is proposed. Specifically, it is as follows. The key (here, it is called a terminal key) of a proper is stored in the computer, and the key and decoder are protected also from the user. A software provider creates the key data which enciphered the used software key with the terminal key while enciphering software with the key (here, it is called a software key) of a proper. At the time of sale, it provides by making into a group the software and key data which were enciphered by the user. since key data encipher a software key with a terminal key -- a specific calculating machine -- only by being, key data can be decoded and a software key can be acquired. And software enciphered using this software key can be decoded and performed.

[0006] The 2nd approach is charged to use of software and distribution of software is taken as no charge. Although it can consider that the base of a view over a certain accounting from the former is the approach of being (a candidate for circulation = accounting) and charging to the acquisition action of software, it is based on the idea that the direction made (applicable to use = accounting) is suitable for digital information offer service, instead of making circulation into no charge in this approach. There is a method called a ″superdistribution″ as an example of this approach. In addition, a superdistribution is detailed in the following reference.

- Woods Ryoichi and Shuichi Tashiro: ″the proposal of a software service system (SSS)″, the Institute of Electronics, Information and Communication Engineers paper magazine Vol.J70D, No.1, and pp.70-81. - Ryoichi Mori, Masaji Kawahara:″Superdistribution : The Concept and the Architecture″ Trans. of IEICE Vol.E73, No.7, pp.1133-1146

The basic concept of a superdistribution is as follows.

(1) An information user can obtain most digital information for free. That is, the gestalt which gets a copy from people besides purchasing from a dealer is also allowed.

(2) The equipment which performs accounting management is built in an information user's terminal, and whenever it actually uses information, it is recorded on accounting equipment. That is, it is charged according to the amount used.

(3) An information user purchases the data (called a common credit) which express informational available frequency with a prepaid method or a credit method, and can use digital information by passing the common

credit to a terminal.

[0007] Thus, by building the structure which can be charged to a use action, the aim of a superdistribution makes it possible it not only to realize protection of copyrights, but to lower a distribution cost extremely and to hold down a substantial software unit price remarkably low by using positively the description of the digital information which degradation from the information on original does not produce even if it copies.

[0008] In a superdistribution, it becomes most important how the structure which can be charged whenever it uses software is realized. As an example, the software distributed consists of two of programs which performs accounting management to the body of software, and its executive operation, and where all are enciphered, it circulates. The module which performs accounting management exists in a user calculating machine, and the module decodes encryption software and starts the accounting program attached to software. An accounting program supervises the operating condition of distribution software, and whenever a charged action occurs, it reduces a common credit. If it is not beyond a value with a common credit, it prevents from starting software. In order to reboot software, a service center is accessed by the communication line and the credit information on a certain frame is purchased. The module of this accounting management must be protected from a user's unauthorized use. Moreover, in the superdistribution, since it assumes that the same encryption software operates at every terminal only by passing the copy itself, the cryptographic key common to every accounting module shall have been memorized.

[0009] As mentioned above, the technique which makes the protection of copyrights to software possible from the former is examined. However, the protection-of-copyrights technique devised to such software has the field which is not enough, when diverting to other digital information as it is is considered. For example, the dubbing edit in a clipping of the report in a newspaper or a video image etc. is the protection of copyrights and the problem of accounting about the so-called secondary use of digital information. That is, since the above-mentioned superdistribution is not taking secondary use of digital information into consideration, it is very difficult the superdistribution to apply to the actual information distribution system by which secondary use will be performed daily. Of course, although a copyright person's profits will be protected if secondary use is forbidden, on the other hand, a user's freedom will be restricted greatly.

[0010] Moreover, this point is not guaranteed, although there should be a possibility that damage may affect the whole system, in the system which unifies informational use and informational accounting like a superdistribution when a protective device is torn.

[0011]

[Problem(s) to be Solved by the Invention] As explained above, the conventional information distribution system was not enough as the technique of the protection of copyrights or accounting to informational secondary use. Moreover, in the system which unifies informational use and informational accounting, if the protective device which stores the decode key etc. should have been torn, there was a possibility that damage might affect the whole system.

[0012] This invention is made in view of the above-mentioned situation, and though it not only performs distribution of charged digital information from a supply station, but the secondary distribution between the terminals which already acquire the digital information should also be possible and the physical safety of a terminal unit should no longer be guaranteed, damage aims at offering the information distribution system and the information distribution approach of being less than except the terminal unit. Moreover, the distribution of digital information itself considers as onerous, and it aims at offering the information distribution system and the information distribution approach of charging the utilization time of digital information.

[0013]

[Means for Solving the Problem] In order to attain the above-mentioned purpose in this invention (claim 1) While consisting of signal transduction media which connect between the information supply station which distributes digital information, two or more information terminals which receive said digital information, and said information supply station and said two or more information terminals In the information distribution system which distributes said digital information distributed from said information supply station between each information terminal in 2nd order said information supply station The encryption digital information which enciphered this digital information using the 1st cryptographic key assigned to the proper for said every digital information, It has a means to output the encryption distribution key which enciphered the 1st decode key corresponding to this 1st cryptographic key using the 2nd cryptographic key assigned at the proper to said information terminal which should transmit this encryption digital information to said signal transduction medium. An input means by which said each of information terminal inputs said encryption digital information transmitted through said signal transduction medium from said information supply station or said other information terminals, and said encryption distribution key, A decode means to decode said encryption digital information using said 1st decode key obtained by this decode after decoding said encryption distribution key using the 2nd decode key of the proper corresponding to said 2nd cryptographic key, After decoding said encryption distribution key using said 2nd decode key, said 1st decode key obtained by this decode An encryption distribution key conversion means to encipher using said 2nd cryptographic key assigned at the proper to said another information terminal which should transmit said encryption digital information, It is characterized by having an output means to output said encryption distribution key obtained by this encryption distribution key conversion means, and said encryption digital information to said signal transduction medium.

[0014] An edit means for said each of information terminal to edit preferably said encryption digital information acquired by said decode means, An available frequency information storing means to store the available frequency information updated whenever it uses the digital information decoded by said encryption digital information or said decode means, While generating record of the use information according to the decode action of said encryption digital information by said decode means, and the edit action of said digital information by said edit means It is characterized by having further the use management tool which updates said available frequency information stored in said available frequency information storing means according to said decode action and said edit action.

[0015] Moreover, said decode means and said encryption distribution key conversion means are preferably characterized by being prepared in the field physically protected from the exterior. Moreover, the information supply station which distributes digital information in this invention (claim 4), While consisting of signal transduction media which connect between two or more information terminals which receive said digital information, and said information supply station and said two or more information terminals In the information distribution system which distributes said digital information distributed from said information supply station between each information terminal in 2nd order said information supply station The 1st cryptographic key assigned to the proper for said every digital information The encryption distribution key which enciphered the 1st decode key corresponding to this 1st cryptographic key using the 2nd cryptographic key assigned at the proper to said information terminal which should transmit the encryption digital information which used and enciphered this digital information, and this encryption digital information, It has a means to output only this encryption distribution key to said signal transduction medium. Or said each of information terminal Said encryption digital information transmitted from said information supply station through said signal transduction medium, and said encryption distribution key Or an input means to input said encryption distribution key transmitted from said encryption digital information transmitted from said other information terminals, and said information supply station, A decode means to decode said encryption digital information using said 1st decode key obtained by this decode after decoding said encryption distribution key using the 2nd decode key of the proper corresponding to said 2nd cryptographic key, It is characterized by having an output means to output said encryption digital information to said signal transduction medium.

[0016] Said information supply office is preferably equipped further with a means to record the distribution action of said encryption distribution key to said each of information terminal. Said each of information terminal The edit means for editing said encryption digital information acquired by said decode means, An available frequency information storing means to store the available frequency information updated whenever it uses the digital information decoded by said encryption digital information or said decode means, While generating record of the use information according to the decode action of said encryption digital information by said decode means, and the edit action of said digital information by said edit means It is characterized by having further the use management tool which updates said available frequency information stored in said available frequency information storing means according to said decode action and said edit action.

[0017] Moreover, it is preferably characterized [which was prepared in the field physically protected from the exterior] by said decode means. On the other hand, by this invention (claim 7), while the 1st information terminal receives distribution of digital information In the information distribution approach of distributing carrier beam digital information to the 2nd information terminal in 2nd order The encryption digital information which enciphered this digital information using the 1st cryptographic key assigned to the proper for said every digital information, The input step which inputs the encryption distribution key which enciphered the 1st decode key corresponding to this 1st cryptographic key using the 2nd cryptographic key assigned to said 1st information terminal at the proper, The decode step which decodes said encryption distribution key using the 2nd decode key of the proper corresponding to said 2nd cryptographic key, The encryption step enciphered using said 2nd cryptographic key to which said 1st decode key obtained by this decode step was assigned by said 2nd information terminal at the proper, It is characterized by having the output step which outputs said encryption distribution key obtained at this encryption step, and said encryption digital information.

[0018] Moreover, in this invention (claim 8), while the 1st information terminal receives distribution of digital information In the information distribution approach of distributing carrier beam digital information to the 2nd information terminal in 2nd order The 1st cryptographic key assigned to the proper for said every digital information The input step which inputs the encryption distribution key which enciphered the 1st decode key corresponding to this 1st cryptographic key using the 2nd cryptographic key assigned at the proper to the encryption digital information which used and enciphered this digital information, and said 1st information terminal, It is characterized by having the step which performs at least one side of the processing which outputs the processing which decodes said encryption distribution key using the 2nd decode key of the proper corresponding to said 2nd cryptographic key, and said encryption digital information.

[0019]

[Function] In invention of claim 1, the 2nd cryptographic key and the 2nd decode key according the 1st cryptographic key and the 1st decode key to a proper in the digital information to distribute are assigned to a proper at a proper. [according to a public key cryptosystem in allocation and each information terminal] In addition, the 1st cryptographic key and the 1st decode key may use any of a public key cryptosystem and a conventional encryption system, and two keys become the same thing when based on a conventional encryption system.

[0020] In an information supply station, in case a receipt information terminal decodes encryption digital information, digital information delivers the encryption distribution key enciphered by the 2nd cryptographic key of an accepting-station proper which described the 1st required decode key above, while enciphering by the 1st cryptographic key of a proper, and it generating encryption digital information and distributing this to a receipt information terminal.

[0021] Moreover, while distributing encryption digital information to other information terminals as it is from the information terminal which already received distribution of encryption digital information, it reenciphers to other information terminals, and the encryption distribution key enciphered for [which was obtained from the information supply station / concerned] information terminals is transmitted to it.

[0022] the 1st decode key with which the accepting station was enciphered -- this terminal -- the 2nd decode key of a proper -- decoding -- this -- after taking out the 1st decode key, the digital information enciphered using this 1st decode key is decoded.

[0023] Here, while encryption digital information can be fundamentally distributed without a limit in this invention, only the information terminal which gained the encryption distribution key which enciphered the 1st decode key corresponding to the 1st cryptographic key used for encryption of this encryption digital information by the 2nd cryptographic key of a proper in the end of a local is able to decode encryption digital information.

[0024] Therefore, it is possible it not only to distribute digital information from an information supply station, but to already distribute to the information terminal which is not so in 2nd order from the information terminal which has received an information supply station to distribution, protecting copyright.

[0025] Moreover, when the physical safety of a specific information terminal is no longer guaranteed, damage does not reach other than the information terminal, but processing of specification of the information terminal, renewal of a key, etc. can also be performed easily. That is, in this invention, the cryptographic key assigned to the proper for each information terminal of every is built in. For this reason, even if the cryptographic key which a certain terminal was torn and was built in is known outside, only the replica of a specific terminal becomes the situation existing [two or more]. Therefore, although not justly charged to the information distributed for the torn specific terminals, accounting to the other information functions normally. Furthermore, what is necessary is just to be able to specify a terminal from the torn key and to update the key of the terminal, although it is necessary in such the condition to make the key into use impossible when the torn key is specified. On the other hand, it is very difficult, although it will be necessary to update the cryptographic key of all terminals when the same cryptographic key is built in all information terminals like before.

[0026] Moreover, if the equipment which performs accounting management is built in in an information terminal, for example like invention of claim 2 and a use condition is managed with the equipment, it can charge normally also to edit actions, such as logging of distribution information and a copy.

[0027] Moreover, in invention of claim 4, peculiar to the digital information to distribute, the 1st cryptographic key and the 1st decode key are assigned to a proper, and the 2nd cryptographic key and the 2nd decode key are assigned to allocation and each information terminal at a proper. In addition, the 1st cryptographic key and the 1st decode key may use any of a public key cryptosystem and a conventional encryption system, and two keys become the same thing when based on a conventional encryption system. Moreover, the 2nd cryptographic key and the 2nd decode key become the same thing when based on a conventional encryption system.

[0028] In an information supply station, in case a receipt information terminal decodes encryption digital information, digital information delivers the encryption distribution key enciphered by the 2nd cryptographic key of an accepting-station proper which described the 1st required decode key above, while enciphering by the 1st cryptographic key of a proper, and it generating encryption digital information and distributing this to a receipt information terminal.

[0029] Moreover, encryption digital information is distributed to other information terminals as it is from the information terminal which already received distribution of encryption digital information. In this case, a different point from invention of claim 1 is a point which surely delivers the encryption distribution key for receipt information terminals from an information supply station to other information terminals.

[0030] the 1st decode key with which the accepting station was enciphered -- this terminal -- the 2nd decode key of a proper -- decoding -- this -- after taking out the 1st decode key, the digital information enciphered using this 1st decode key is decoded.

[0031] Here, while encryption digital information can be fundamentally distributed without a limit in this invention, only the information terminal which gained the encryption distribution key which enciphered the 1st decode key corresponding to the 1st cryptographic key used for encryption of this encryption digital information by the 2nd cryptographic key of a proper in the end of a local is able to decode encryption digital information.

[0032] Therefore, it is possible it not only to distribute digital information from an information supply station, but to already distribute to the information terminal which is not so in 2nd order from the information terminal which has received an information supply station to distribution, protecting copyright.

[0033] Moreover, like invention of claim 1, when the physical safety of a specific information terminal is no longer guaranteed, damage does not reach other than the information terminal, but processing of specification of the information terminal, renewal of a key, etc. can also be performed easily.

[0034] Moreover, in order to build in the equipment which performs accounting management in an information terminal, for example like invention of claim 5 and to manage a use condition with the equipment, it can charge normally also to edit actions, such as logging of distribution information and a copy.

[0035] Moreover, in order to decode the distributed information, it is necessary to access an information supply office, and according to this invention, it becomes possible by recording the access action to carry out accounting management in an information supply office.

[0036] On the other hand, in invention of claim 7, the 1st cryptographic key and the 1st decode key are assigned at a proper to the digital information distributed, and the 2nd cryptographic key and the 2nd decode key by the public key cryptosystem are assigned [a proper] to an information terminal at a proper. In addition, the 1st cryptographic key and the 1st decode key may use any of a public key cryptosystem and a conventional encryption system, and two keys become the same thing when based on a conventional encryption system.

[0037] In case digital information decodes the encryption digital information enciphered by the 1st cryptographic key of a proper, and this encryption digital information, the encryption distribution key enciphered by the 2nd cryptographic key of the terminal proper concerned which described the 1st required decode key above is distributed to an information terminal.

[0038] Moreover, when having already received distribution of encryption digital information, this information terminal reenciphers to other information terminals to them, and can transmit the encryption distribution key enciphered for [which has already been gained / concerned] information terminals to it to them while it distributes the encryption digital information concerned as it is to other information terminals.

[0039] the 1st decode key with which the information terminal was enciphered -- this terminal -- the 2nd decode key of a proper -- decoding -- this -- after taking out the 1st decode key, the digital information enciphered using this 1st decode key can be decoded.

[0040] Here, while encryption digital information can be fundamentally distributed without a limit in this invention, only the information terminal which gained the encryption distribution key which enciphered the 1st decode key corresponding to the 1st cryptographic key used for encryption of this encryption digital information by the 2nd cryptographic key of a proper in the end of a local is able to decode encryption digital information.

[0041] Therefore, protecting copyright, when an information terminal not only can receive distribution of digital information, but has already received distribution, it can distribute the digital information concerned to other information terminals in 2nd order.

[0042] Moreover, when the physical safety of a specific information terminal is no longer guaranteed, damage does not reach other than the information terminal, but processing of specification of the information terminal, renewal of a key, etc. can also be performed easily.

[0043] Moreover, in invention of claim 8, the 1st cryptographic key and the 1st decode key are assigned at a proper to the digital information distributed, and the 2nd cryptographic key and the 2nd decode key are assigned [a proper] to each information terminal at a proper. In addition, the 1st cryptographic key and the 1st decode key may use any of a public key cryptosystem and a conventional encryption system, and two keys become the same thing when based on a conventional encryption system. Moreover, the 2nd cryptographic key and the 2nd decode key become the same thing when based on a conventional encryption system.

[0044] In case digital information decodes the encryption digital information enciphered by the 1st cryptographic key of a proper, and this encryption digital information, the encryption distribution key enciphered by the 2nd cryptographic key of the terminal proper concerned which described the 1st required decode key above is distributed to an information terminal.

[0045] Moreover, encryption digital information can be distributed to other information terminals as it is from the information terminal which already received distribution of encryption digital information. the 1st decode key with which the accepting station was enciphered -- this terminal -- the 2nd decode key of a proper -- decoding -- this -- after taking out the 1st decode key, the digital information enciphered using this 1st decode key is decoded.

[0046] Here, while encryption digital information can be fundamentally distributed without a limit in this invention, only the information terminal which gained the encryption distribution key which enciphered the 1st decode key corresponding to the 1st cryptographic key used for encryption of this encryption digital information by the 2nd cryptographic key of a proper in the end of a local is able to decode encryption digital information.

[0047] Therefore, it not only can receive distribution of digital

information, but an information terminal can be distributed to the information terminal which is not so in 2nd order from the information terminal which has already received distribution from the information supply office, protecting copyright.
[0048] Moreover, like invention of claim 1, when the physical safety of a specific information terminal is no longer guaranteed, damage does not reach other than the information terminal, but processing of specification of the information terminal, renewal of a key, etc. can also be performed easily.
[0049]
[Example] Hereafter, the example of this invention is explained, referring to a drawing. The information distribution structure of a system concerning one example of this invention is shown in drawing 1 . This information distribution system is suitable when it is going to realize an information distribution gestalt which distributes information to a user gratuitously and charges informational utilization time for the first time. While receiving distribution of the information supply station 101 which offers information distribution service, the communication system (signal transduction medium) 102 with which informational transfer is presented, and information it is as it is about carrier beam information -- it is -- it consists of a service center 104 which carries out management of the information terminal 103 which can be processed and can be distributed in 2nd order, and the cryptographic key used by this system so that it may mention later etc.
[0050] The distribution information treated by this example shall include visual-and-auditory-senses-information, such as document (and still picture) information which is the format in which the text, the voice and the image, or these which were digitized were intermingled, for example, is represented by publications, such as a newspaper and a magazine, and music, a movie.
[0051] The information supply station 101 distributes information on charged (especially work) according to a demand of the information terminal 103 etc. The number of the information supply stations 101 prepared in the information distribution system concerned is arbitrary.
[0052] The information terminal 103 has a function for editing the information other than the function which displays the information which receives informational distribution from the information supply station 101, and which was functioned and distributed, communication facility with other information terminals, etc. and it is as it is about the received information if needed -- it is -- it can be processed and other information terminals 103 can be passed. The number of the information

terminals 103 is arbitrary.

[0053] The service center 104 has managed the database of the cryptographic key of each information terminal 103, and is accessed from the information supply station 101 or the information terminal 103 if needed.

[0054] Transfer of the information between each station 101,103,104 is performed through communication system 102. In addition, it is also possible to use the media of what kind of gestalt for transfer of distribution of the digitized charged information, the required decode key mentioned later, and to use the broadcast and the record media other than the usual communication line (for example, CD-ROM, a floppy disk, a memory card, etc.). Moreover, it is also possible to constitute so that a signal transduction medium which is mutually different with charged information and a required decode key, for example may be used. Suppose that the usual communication line is used as communication system 102 in this example.

[0055] At this example, in order to realize the unjust acquisition of distribution way data and the protection of an alteration in a communication line etc., charged information is distributed in the condition of having been enciphered. The information supply office 101 sets up the group (however, a cryptographic key and a decode key may be the same) of a different cryptographic key for every distribution information, and a decode key (it is hereafter called a distribution key), and enciphers distribution information by the cryptographic key. The information terminal 103 mounts the decode function and can decode the distribution information enciphered when acquiring the distribution key.

[0056] Moreover, in this example, in order to provide a user with the use gestalt which employed the description of digital information efficiently, an informational copy considers as freedom (no charge), and does actions, such as a display and viewing and listening, the charge. Moreover, the action (for example, it is called informational secondary use below action; that starts informational [a part of] and is compounded with other data) which edits all or a part of distributed charged information is done to accepting without forbidding, instead is charged to informational secondary use.

[0057] Here, in order to charge to an informational use action instead of charging the informational distribution itself, the device in which distinguish informational use and it charges according to the result is needed. First, as an approach of realizing an accounting device, the following two approaches can be considered, for example.

[0058] one approach -- the information supply station 101 -- the information terminal 103 of specification [a distribution key] -- the action distributed for turning is supervised and record of this action is taken. Other approaches equip each information terminal 104 each with the device (it is hereafter called an accounting module) which controls the amount of information use of the device and user who detect an informational decode action and an informational edit action.

[0059] Although the former approach can be charged to the distribution action of the charged information from the information supply office 101, to the ability not to charge, the other action (for example, distribution of the charged information on information terminal 103 comrades and informational secondary use) makes the informational distribution itself no charge, and when information is used for the latter approach, it can charge it.

[0060] In this example, the latter approach which can be charged to the information use action itself is used. in addition, although it is alike and an accounting module sets, as long as it operates normally, and it can control the amount of information use, while the latter approach needs to protect the accounting module itself from an attack for that purpose, in order that an information offer side may, in addition, grasp the amount of the work unit used, a means to collect the use records in an accounting module is needed. By this example, the method of collecting the configuration of the accounting module shown by the ″superdistribution system″ and use records is applicable about these points. They are the following structure when it explains briefly. The available frequency information (it is equivalent to data and the credit which are recorded on the prepaid card) reduced whenever a user uses charged information exists, and this is recorded on the medium (for example, IC card) which cannot be operated from the user. When the available frequency information in a medium runs short, it becomes impossible to perform decode of distribution information etc. by control of an accounting module. If a user returns the medium to an information offer side (this example information supply station 101), an information offer side will increase available frequency and will deliver this to a user again. By writing in use record of a work unit by actuation of an accounting module in this medium, it is an information offer side and use records can be collected with renewal of frequency information. Moreover, use record can also be transmitted by the communication line. Unless a reception signal is received from an information offer side, it constitutes from a gestalt by the communication line so that informational use may become impossible by control of an accounting

module.
[0061] Next, the example of a configuration of the information terminal 103 which realizes the function explained above is explained, referring to drawing 2 . As shown in drawing 2 , the information terminal 103 is equipped with the accounting module 201, the user memory 202, a display 203, a command input area 204, the secondary storage interface section 205, the number storage interface section 206 of availabilities, and the communications department 207.
[0062] Among these, the accounting module 201 is a module protected physically, and as shown in drawing 3 , the execution control section 301, the code machine / decoder 302, the key storage section 303, the accounting Management Department 304, and a guarded memory 305 are formed in the interior. Although various level exists in the approach of protecting an accounting module physically, the approach of constituting the whole module with the 1 chip LSI, the approach of closing the whole module other than an input output line by resin, the method of preparing a physical unlawful access detection device in a module, and when some examples are given, and unlawful access is detected further, there is the approach of eliminating the memory content in a module etc. In addition, physical unlawful access assumes the action which carries out direct probing of the parts other than an input output line, and the concrete detection device is reference. Ryoichi Mori, Masaji Kawahara: ″Superdistribution:The Concept and the Architecture″, Trans.of IEICE, Vol.E73, No.7, pp.1133-1146 It is stated.
[0063] While the accounting module 201 has a function for editing the information which enciphers the information which decodes the enciphered information, and which was functioned and decoded and which was functioned and decoded and charging it to informational use (decode and a display, and edit), when it cannot charge, the control which forbids informational use carries out. In addition, fundamentally, the decoded distribution information (plaintext) is held at the guarded memory 305 of the accounting module 201 interior, and cannot be directly read from the exterior. However, when informational secondary use is carried out so that it may mention later, a part of distribution information (plaintext) decoded after charging is outputted to the exterior of the accounting module 201 concerned.
[0064] The user memory 202 is for storing the enciphered information. A command input area 204 is for receiving the command from a user, and can use a keyboard, the so-called mouse, etc. as an input device. Decode presenting of distribution information, a demand of distribution information (to information supply station 101), informational (end of

the other end 103) transmission, informational (from end of the other end 103) reception, informational edit (secondary use), etc. are prepared for the command used at the information terminal 103.

[0065] A display 203 carries out a screen display of the decoded distribution information, or displays the screen corresponding to each command, for example, an edit display and a communication link screen. The number storage interface section 206 of availabilities is an interface which holds the number storage 208 of availabilities for recording the number of availabilities. If an IC card is used for the number storage 208 of availabilities, it is desirable and IC card reader can be used for the number storage interface section 206 of availabilities in this case.

[0066] The communications department 207 is a communication interface for transmitting and receiving distribution information etc. with the exterior. That is, each information terminal 103 is connected to communication system 102 through this communications department 207.

[0067] The secondary storage interface section 205 is an interface which holds the secondary storage (not shown) for memorizing the distributed information. It is desirable when a hard disk, a floppy disk, etc. which can memorize information in large quantities are used for secondary storage.

[0068] Hereafter, the example of operation in the above-mentioned configuration is explained roughly. The charged information distributed as mentioned above is enciphered. At the information terminal 103, if the decode viewing command of distribution information is received, before decoding information, the accounting Management Department 304 in the accounting module 201 will investigate the balance frequency in the number storage 208 of availabilities first. If it is more than the frequency that needs balance frequency for a decode display, "the signal which can be performed" will be sent to the execution control section 301. In response, the execution control section 301 transmits distribution information to the guarded memory 305 in the accounting module 201 from secondary storage (not shown) or the user memory 202.

[0069] In addition, when distribution information is extensive, you may make it transmit only the circumference of the field actually displayed. For example, if it is the information on a magazine etc., and only the data of the page size which can be displayed by the display 203 will be transmitted and the data corresponding to whenever [of an input of the page turning-over command from a user] will be transmitted, since processing is accelerable, it is effective.

[0070] The execution control section 301 is decoded by the code function of a code machine / decoder 302 using the decode key in which the information in the accounting module 201 is stored by the key storage section 303, and is stored in a guarded memory 305. In a display 203, the contents of the guarded memory 305 are accessed and a screen display etc. is performed.

[0071] By the accounting module 201, the number of pages which indicated, for example by decode is counted, and the displayed frequency per page is reduced from the frequency information in the frequency storage 208 at the accounting Management Department 304 each time. When the frequency storage 208 is removed, when not succeeding in a cut, the execution control module 301 in the accounting module 201 processes clearing the contents of the guarded memory 305 etc., and it prevents from using distribution information.

[0072] Here, informational secondary use can be performed at the information terminal 103. As secondary use of this information, the clipping action to the information currently displayed is typical. In this case, preservation to range assignment / file will be performed as a user command. And with reference to frequency information, if it is reducible, it will be performed, the accounting module 201 calculates the amount of accounting to a clipping of the field from a range assignment command, when that is not right, it displays an error message, and it is made not to perform it. Tariff information required for count of the amount of accounting is attached for every distribution object, and contains data, such as "display tariff [per page]", and a clipping tariff per page."

[0073] In addition, it is also possible to add the information which shows that secondary use is permitted / forbidden about a distribution object, to follow this information, and to constitute so that secondary use may be permitted / forbidden. When secondary use is forbidden, the decoded distribution information (plaintext) is not outputted to the exterior of the accounting module 201.

[0074] The above is the configuration and function of the information terminal 103. Next, the method of information distribution (primary distribution and secondary distribution) used in the information distribution system which has the configuration mentioned above is explained about two kinds of things.

[0075] Drawing 4 is the configuration that the 1st information distribution method was shown, and used the conventional encryption system for informational delivery, and it used the public key cryptosystem for the transfer of a distribution key. The private key (decode key) of a proper is memorized by the key storage section 303 inside [accounting module 201] each information terminal 103, respectively. On the other hand, the public key (cryptographic key) is exhibited in the accessible condition from the information supply station 101 and each information terminal 103. Hereafter, in explanation of this method, the private key of information terminal #i which is going to receive informational distribution from the information supply station 101 is made into SK_i, and a public key is made into PK_i.

[0076] Information terminal #i holds the "public key certificate" with which the service center 104 performed the digital signature to the data which carry out by installing a open database in the service center 104 of drawing 1 , or wove in by making a public key and ID information on information terminal #i into a group, and whenever management of a public key is a demand, it may be performed by exchanging a public key certificate.

[0077] In the information supply office 101, "distribution key WK_P" of a proper is set to every information P, and information is enciphered with a distribution key. A common use code with high-speed processing speed is used for the cipher system at this time. This encryption distribution information is made to describe it as C_P=WK_P (P). Information terminal #i can restore the usual distribution information based on encryption distribution information by obtaining distribution key WK_P.

[0078] Hereafter, the procedure of primary distribution of the information from the information supply office 101 to information terminal #i is explained, referring to the flow chart of drawing 5 . In addition, in the information supply station 101, Information P shall be enciphered by distribution key WK_P of a proper, and it shall already have stored in the storage which does not link and illustrate encryption distribution information C_P and distribution key WK_P.

[0079] The demand of distribution of Information P occurs from information terminal #i to the information supply station 101 in the beginning (step S1). The information supply station 101 acquires public key PK_i corresponding to information terminal #i of a requiring agency from a service center 104 (step S2).

[0080] Performing Challenge Handshake Authentication Protocol between the information supply station 101 and information terminal #i, the information supply station 101 checks the justification of information terminal #i (step S3). The fact that the partner terminal possesses private key SK_i is checked, the side (here information terminal #i) attested [delivery and] enciphers the random number by private key SK_i, for example, returns an inspection side (here information supply station 101) to a random number, and Challenge Handshake Authentication Protocol here should just inspect that the random number which carried out [the random number] inverse transformation and was transmitted by public key PK_i appears in an inspection side.

[0081] When it succeeds in authentication (in the case [Step S4] of Yes), the information supply station 101 searches from storage distribution key WK_P used for encryption information C_P (step S6), and enciphers this distribution key WK_P with the public key of information terminal #i (step S7). Thus, while calling the information generated an encryption distribution key, it will be written as D_iP=PK_i (WK_P).

[0082] Next, encryption information C_P of the information P to distribute is searched (step S8), and encryption distribution information C_P and encryption distribution key D_iP are distributed to information terminal #i (step S9).

[0083] Information terminal #i which received encryption distribution information C_P and encryption distribution key D_iP by the above-mentioned primary distribution can take out distribution key WK_P from encryption distribution key D_iP by the decode function of a code machine / decoder 302 using private key SK_i stored in the key storage section 303 in the accounting module 201, and can decode encryption distribution information C_P at distribution key WK_P further. Distribution key WK_P does not appear in the accounting module 201 exterior of information terminal #i, but at the time of preservation of distribution information, linking of encryption distribution information C_P and its encryption distribution key D_iP is carried out, and it is stored.

[0084] In addition, it is also possible to start information distribution by notifying distribution of Information P to information terminal #i from the information supply station 101 instead of starting information distribution by requiring distribution of Information P of the information supply station 101 from information terminal #i at step S1.

[0085] Next, the procedure of secondary distribution of the information from information terminal #i to information terminal #j is explained, referring to the flow chart of drawing 6 . In addition, information terminal #i has received encryption distribution information C_P corresponding to the distribution information P from the information supply station 101, shall carry out linking of encryption distribution information C_P and its encryption distribution key D_iP, and shall already have stored it.

[0086] The demand of the distribution of Information P to information terminal #i from information terminal #j to the beginning occurs like the case of the primary distribution from the information supply station 101 (step S11). Information terminal #i acquires public key PK_j corresponding to information terminal #j of a requiring agency from a service center 104 (step S12).

[0087] Next, Challenge Handshake Authentication Protocol is performed between information terminal #i and j by the same approach as the case of primary distribution (step S13). In addition, activation of the Challenge Handshake Authentication Protocol of this step S13 may be excluded.

[0088] When it succeeds in authentication (in the case [Step S14] of Yes), information terminal #i searches encryption distribution key D_iP (step S16). Next, encryption distribution key D_jP passed to information terminal #j based on searched encryption distribution key D_iP is generated (step S17). First, information terminal #i inputs encryption distribution key D_iP and public key PK_j of information terminal #j into the accounting module 201. By the accounting module 201, encryption distribution key D_iP to distribution key WK_P for information terminal #i is taken out, and encryption distribution key D_jP=PK_j (WK_P) for information terminal #j further enciphered by public key PK_j corresponding to information terminal #j is generated.

[0089] Next, encryption information C_P of the information P to distribute is searched (step S18), and encryption distribution information C_P and encryption distribution key D_jP are distributed to information terminal #j (step S19).

[0090] By the above-mentioned secondary distribution, distribution key WK_P can be taken out from encryption distribution key D_jP by the decode function of a code machine / decoder 302 using private key SK_j which has stored in the key storage section 303 in the accounting module 201 information terminal #j which received ******** in encryption distribution information C_P and encryption distribution key D_jP, and encryption distribution information C_P can be further decoded at distribution key WK_P. Distribution key WK_P does not appear in the accounting module 201 exterior of information terminal #j, but at the time of preservation of distribution information, linking of encryption distribution information C_P and its encryption distribution key D_jP is carried out, and it is stored.

[0091] In addition, it is also possible to start information distribution by notifying distribution of Information P to information terminal #j from information terminal #i instead of starting information distribution by requiring distribution of Information P of information

terminal #i from information terminal #j at step S11.
[0092] Although transform processing of an encryption distribution key like creation of encryption distribution key D_iP to D_jP is needed at every secondary distribution by this method, encryption distribution information C_P itself can be distributed as it is. Usually, as for the size of Information P, it is effective that it can use without re-enciphering encryption distribution information C_P since it is very large compared with distribution key WK_P.
[0093] In addition, although the same WK_P will be enciphered by two or more cryptographic keys when a RSA (Rivest-Shamir-Adleman) code is used as public key encryption, in such a case, existence of the attacking method is known. The example of the attacking method is detailed in the following reference.
**J. Hastad, ″On using RSA with low exponent in a public key network″, Lecture Notes in Computer Science: Advances in Cryptology - CRYPTO'85 proceedings Springer-Verlag pp.403-408
Then, when using RSA cryptograph as public key encryption, since it is larger than the size of the distribution key in a common use code, for example, if the size of the plaintext which can be enciphered as 1 block of RSA generates a different random number R for every distribution session and R||WK_P (however, || means connection of data) is used as a plaintext of an encryption distribution key, it is desirable.
[0094] Next, the 2nd information distribution method is explained. Drawing 7 shows the 2nd information distribution method, and is the configuration that informational delivery and a transfer of a distribution key used the conventional encryption system. However, a public key cryptosystem may be used for a transfer of a distribution key like the 1st information distribution method.
[0095] The private key of a proper is memorized by each information terminal 103 at the key storage section 303 of the accounting module 201 interior. In this case, a private key is used for both encryption and a decryption for a common use code. Hereafter, the private key of information terminal #i is made into K_i in explanation of this method.
[0096] The service center 104 has managed the database of private key K_i, and private key K_i corresponding to each information terminal 103 can grasp only a service center 104. The information supply station 101 accesses a service center 104, and can acquire private key information. However, in this example, private key information shall be unacquirable from the information terminal 103.
[0097] In the information supply office 101, ″distribution key WK_P″ of a proper is set to every information P, and information is enciphered

with a distribution key. A common use code with high-speed processing speed is used for the cipher system at this time. This encryption information is made to describe it as C_P=WK_P (P). Information terminal #j can restore the usual distribution information based on encryption distribution information by obtaining distribution key WK_P.

[0098] Hereafter, the procedure of primary distribution of the information from the information supply office 101 to information terminal #i is explained, referring to the flow chart of drawing 8 . In addition, in the information supply station 101, Information P shall be enciphered by distribution key WK_P of a proper, and it shall already have stored in the storage which does not link and illustrate Information P, encryption distribution information C_P, and distribution key WK_P.

[0099] The demand of distribution of Information P occurs from information terminal #i to the information supply station 101 in the beginning (step S21). The information supply station 101 acquires public key K_i corresponding to information terminal #i of a requiring agency from a service center 104 (step S22).

[0100] The information supply station 101 performs Challenge Handshake Authentication Protocol between information terminal #i, and checks the justification of information terminal #i (step S23). The fact that the partner terminal possesses private key K_i to be sure is checked, the side (here information terminal #i) attested [delivery and] enciphers the random number by private key K_i, for example, returns an inspection side (here information supply station 101) to a random number, and Challenge Handshake Authentication Protocol here should just inspect that the random number which carried out [the random number] inverse transformation and was transmitted by key K_i of terminal #i appears in an inspection side.

[0101] When it succeeds in authentication (in the case [Step S24] of Yes), the information supply station 101 searches from storage distribution key WK_P used for encryption information C_P (step S26), and enciphers this distribution key WK_P with the private key of information terminal #i (step S27). Thus, while calling the information generated an encryption distribution key, it will be written as D_iP=K_i (WK_P).

[0102] Next, encryption information C_P of the information P to distribute is searched (step S28), and encryption distribution information C_P and encryption distribution key D_iP are distributed to information terminal #i (step S29).

[0103] Information terminal #i which received encryption distribution information C_P and encryption distribution key D_iP by the above-mentioned primary distribution takes out distribution key WK_P from encryption distribution key D_iP by the decode function of a code machine / decoder 302 using private key K_i stored in the key storage section 303 in the accounting module 201, and decodes encryption distribution information C_P at distribution key WK_P further. Distribution key WK_P does not appear in the accounting module 201 exterior of information terminal #i, but at the time of preservation of distribution information, linking of encryption distribution information C_P and its encryption distribution key D_iP is carried out, and it is stored.

[0104] In addition, it is also possible to start information distribution by notifying distribution of Information P to information terminal #i from the information supply station 101 instead of starting information distribution by requiring distribution of Information P of the information supply station 101 from information terminal #i at step S21.

[0105] Next, the procedure of secondary distribution of the information from information terminal #i to information terminal #j is explained, referring to the flow chart of drawing 9 . In addition, information terminal #i has received encryption distribution information C_P corresponding to the distribution information P from the information supply station 101, shall carry out linking of encryption distribution information C_P and its encryption distribution key D_iP, and shall already have stored it.

[0106] The demand of the distribution of Information P to information terminal #i occurs from information terminal #j like the case of the primary distribution from the information supply station 101 (step S31). Information terminal #i searches encryption distribution information C_P of Information P (step S32), and transmits information terminal #j ** (step S33). In addition, in distributing encryption distribution information C_P to information terminal #j from information terminal #i, Challenge Handshake Authentication Protocol does not perform information terminal #i between information terminal #j.

[0107] Next, information terminal #j requires encryption distribution key D_jP required for decode of encryption distribution information C_P of the information supply station 101 (step S34). The information supply station 101 acquires private key K_j of information terminal #j from a service center 104 according to this demand (step S35).

[0108] Next, by the same approach as the case of primary distribution, the information supply station 101 performs Challenge Handshake

Authentication Protocol between information terminal #j, and checks the justification of information terminal #j (step S36). In addition, when it distributes an encryption distribution key from the information supply station 101 mentioned later and it takes the approach that information terminal #j is charged, since this step S36 can check whether the distribution place of an encryption distribution key is information terminal #j certainly, it is effective. Moreover, when taking the approach that the utilization time of the information mentioned later is charged for the first time, activation of this Challenge Handshake Authentication Protocol may be excluded.

[0109] When it succeeds in authentication (in the case [Step S37] of Yes), the information supply station 101 searches distribution key WK_P used for encryption information C_P (step S39), enciphers this distribution key WK_P with the private key of information terminal #j, and generates encryption distribution key D_jP (step S40). In addition, D_jP=K_j [an encryption distribution key] (WK_P) is written.

[0110] Next, encryption distribution key D_jP is distributed to information terminal #j (step S41). Information terminal #j which received encryption distribution information C_P and encryption distribution key D_jP by the above-mentioned secondary distribution can take out distribution key WK_P from encryption distribution key D_jP by the decode function of a code machine / decoder 302 using private key K_j stored in the key storage section 303 in the accounting module 201, and can decode encryption distribution information C_P at distribution key WK_P further. Distribution key WK_P does not appear in the accounting module 201 exterior of information terminal #j, but at the time of preservation of distribution information, linking of encryption distribution information C_P and its encryption distribution key D_jP is carried out, and they are stored.

[0111] In addition, it is also possible to start information distribution by notifying distribution of Information P to information terminal #j from information terminal #i instead of starting information distribution by requiring distribution of Information P of information terminal #i from information terminal #j at step S31.

[0112] By this method, although it is a fault that informational use cannot be performed only for secondary distribution information since secondary distribution of only encryption distribution information C_P is possible, secondary encryption distribution information C_P which is a lot of information can be distributed.

[0113] In addition, we decided that encryption information C_P corresponding to the information P to distribute is stored in the user memory 202, secondary storage which is not illustrated of the information terminal 103 in secondary distribution, the information terminal 103 searches encryption information C_P with each above-mentioned information distribution method (steps S18 and S32), and this is distributed (steps S19 and S32). Instead, what enciphered the plaintext which information terminal 103 confidence decoded and was obtained by the cryptographic key (public key) of an accepting station 103 may be distributed as encryption distribution information.

[0114] Moreover, it corrects suitably and drawing 5 and the procedure shown in the flow chart of 6, 8, and 9 can be carried out. As mentioned above, the information terminal 103 of arbitration can acquire the information on desired from the information supply station 101 or other information terminals 103 with the information distribution method mentioned above.

[0115] Next, in the information distribution system by each information distribution method, it explains how it should charge to acquisition (or informational viewing and listening) of charged information, and secondary use of charged information.

[0116] Since distribution by information terminal 103 comrades is performed by the 1st information distribution method shown in drawing 4 in addition to the distribution from the information supply office 101, in order to charge systematically, the method of counting the decode action of charged information by the accounting module 201 built in each information terminal 103, and charging at every decode of charged information is good.

[0117] As the escape, it is also still more possible to be charged only when decoding once first, and to make it not charge to the decode after the 2nd times of the same information. This can realize the serial number of the encryption distribution information decoded once by saving as a list in the accounting module 201.

[0118] In addition, although there is no information supply office 101 in accounting with a direct epilogue, the record can be used for discovery of an unjust terminal etc. by leaving record of information distribution. On the other hand, by the 2nd information distribution method shown in drawing 7 , since it is necessary to surely obtain an encryption distribution key from the information supply office 101 in order to view and listen to charged information, if this action is recorded in the information supply office 101, accounting to the supply action of charged information can be performed. That is, even if it decodes the information distributed once how many times and displays it, let it be a fixed tariff.

[0119] In addition, if the accounting module 201 of information terminal 103 built-in is used, the action which charges at every decode of charged information is also possible, although it leaves record of issue of an encryption distribution key, informational distribution can be made into no charge and all accounting can also be left to the accounting module 201 of information terminal 103 built-in in the information supply office 101. That is, suppose that it does not charge unless it is used even if it receives an encryption distribution key.
[0120] In addition, in the case of which [of the 1st information distribution method and the 2nd information distribution method], processing of the accounting module 201 performs secondary use of charged information. Here, by the 2nd information distribution method shown in the 1st information distribution method and drawing 7 shown in drawing 4 , the private key of a proper is stored in each information terminal 103, and, moreover, the contents of the private key are made secret also to the user of the information terminal 103. However, since the module which performs accounting management exists in a user terminal 103, the module is attacked by the vicious user and a private key may be revealed. How to have revealed private key K_x of information terminal #x temporarily in the system of the 2nd information distribution method of drawing 7 . At this time, information distributed to information terminal #x can be ******(ed) by using that private key K_x. However, since the information distributed to other information terminals cannot be decoded by private key K_x, it is impossible for ******(ing). That is, by this method, even if the private key of a specific information terminal is revealed, information on arbitration cannot necessarily be ******(ed) and damage will not affect the whole system.
[0121] Moreover, although distribution of the information on arbitration can also be received [information terminal #x] to the information supply office 101, if it does in this way, injustice will be revealed from the log of the distribution recorded on the information supply office 101, and the log of the use record collected from actual information terminal #x, and it will become clear that private key K_x was revealed from information terminal #x. In such a case, what is necessary is to make private key K_x into use impossible, and just to update key K_x of information terminal #x.
[0122] Thus, the soundness of a system improves greatly by having turned the key of the information terminal 103 the individual exception. About this point, it is the same also in the system of the 1st information distribution method of drawing 4 . However, since secondary distribution

is performed without mediation of the information supply station 101, this system is insufficient only at the log of the information supply station 101. When secondary distribution is performed, the fact is recorded on both the information terminal 103 of a transmitting side, and the information terminal 103 of a receiving side, and if it will collect by approach which described those use records previously, injustice can be checked by tracing the record.

[0123] The nullification and updating of a subsequent key are the same as the case of a previous system. Here, by each information distribution method mentioned above, although the conventional encryption system was used for informational primary distribution and secondary distribution instead, even if it uses a public key crypto system, the same effectiveness is acquired. In this case, in case an accepting station 103 decodes encryption distribution information, only a required decode key (private key) is used as a distribution key, and the information supply station 101 should just send the information which enciphered this by the cryptographic key (public key) of a proper to the accepting station 103 to this accepting station 103.

[0124] Moreover, as mentioned above, it is also possible to use the broadcast and the record media other than the usual communication line (for example, CD-ROM, a floppy disk, a memory card, etc.) which could use the media of what kind of gestalt for transfer of the information between each station 101,103,104, and were used for it by this example. In addition, since the configuration of each station in this case is clear, detailed explanation is omitted. Moreover, this invention is not limited to each example mentioned above, it is the range which does not deviate from the summary, and can deform variously and can be carried out.

[0125]

[Effect of the Invention] According to the information distribution system concerning this invention, a cryptographic key and a decode key are assigned to each information terminal at a proper at a proper. Since what allocation and digital information enciphered the cryptographic key and the decode key as by the cryptographic key of a proper is distributed to a proper at the digital information to distribute and a decode key required for this is enciphered and delivered by the cryptographic key of a proper to an accepting station It is possible it not only to distribute digital information from an information supply station, but to already distribute to the information terminal which is not so in 2nd order from the information terminal which has received an information supply station to distribution, protecting copyright.

Moreover, when the physical safety of a specific information terminal is no longer guaranteed, damage does not reach other than the terminal unit, but processing of specification of the information terminal, renewal of a key, etc. can also be performed easily.

[0126] Moreover, it can charge also to secondary use of edit of the information on the distributed charge etc. On the other hand, according to the information distribution approach concerning this invention, a cryptographic key and a decode key are assigned to a proper by the information terminal at a proper. Since a cryptographic key and a decode key are assigned at a proper to the digital information distributed, digital information distributes what was enciphered by the cryptographic key of a proper and a decode key required for this is enciphered and delivered by the cryptographic key of a proper to an accepting station It is possible it not only can to receive distribution of digital information, but to distribute this digital information to other information terminals in 2nd order at an information terminal from the information terminal which has already received distribution, protecting copyright. Moreover, when the physical safety of a specific information terminal is no longer guaranteed, damage does not reach other than the terminal unit, but processing of specification of the information terminal, renewal of a key, etc. can also be performed easily.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] Drawing showing the outline configuration of the information distribution system concerning one example of this invention

[Drawing 2] Drawing showing the example of a configuration of the information terminal in this example

[Drawing 3] Drawing showing the example of a configuration of the accounting module in this example

[Drawing 4] Drawing for explaining the 1st information distribution method concerning one example of this invention

[Drawing 5] The flow chart of the primary distribution procedure in this method

[Drawing 6] The flow chart of the secondary distribution procedure in this method

[Drawing 7] Drawing for explaining the 2nd information distribution method concerning one example of this invention

[Drawing 8] The flow chart of the primary distribution procedure in this method

[Drawing 9] The flow chart of the secondary distribution procedure in this method

[Description of Notations]

101 -- information supply station, 102 -- communication system, and 103 -- an information terminal, a 104 -- service center, a 201 -- accounting module, and 202 -- user memory, a 203 -- display, a 204 -- command input area, and 205 -- the secondary storage interface section, 206 -- frequencies storage interface section, the 207 -- communications department, and 208 -- the number storage of availabilities, the 301 -- execution control section, 302 -- code machine / decoder, and 303 -- the key storage section, the 304 -- accounting Management Department, and a 305 -- guarded memory